FOIA, Privacy & Records Management Conference 2009

Date:11/16/2009

System of Records Notice (SORN)

and

Privacy Impact Assessments (PIAs)

Mr. Leroy Jones, Jr. ***Army Privacy Office*** ***(703) 428-6185***
Leroy.Jonesjr1@us.army.mil
Mrs. Margaret Hamrick ***Army Privacy Office*** ***(703) 428-6193***
Margaret.Hamrick@us.army.mil
Ms Cynthia Dixon ***CIO/G-6*** ***(703) 604-2022***
cynthia.dixon@us.army.mil
Ms Cathy Cowan ***CIO/G-6*** ***(703) 602-7432***

System of Record Notice (SORN) and Privacy Impact Assessments (PIAs)

Purpose of this session

- To provide information/guidance on SORNs
- To provide guidance on what NETCOM/9th Sig Accreditation and FISMA
- To provide an understanding of the PIA process
- To provide guidance and training on correctly completing the PIA template DD Form 2930

System of Record

IAW DoD 5400.11-R (Defense Privacy Program)

DL1.24, System of Record (SOR) is a group of any

Records (paper or electronic) under the control of a DoD

Component (Army) from which information is retrieved

by the name of the individual or by some identifying

number, symbol, or other identifying particular assigned

to the individual (such as SSN, date of birth, symbol, etc.).

System of Record Notices (SORN)

Definition

- A description of a group of records that:
  - Under the control of the Agency (Army, etc)
  - Is published in the Federal Register (FR)
  - Authorizes the collection of Personally Identifiable Information (PII)
  - If records are not retrieved by an individuals name or personal identifier, they are not a PA system of records

PII &System of Record Notices

- **OMB Memorandum, M-07-16, 22 May 2007 states:**

  - Personally Identifiable Information (PII) refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.*

Responsibilities

- **PRIVACY OFFICERS:**
  - A Privacy Official is appointed at Command levels throughout the Army
  - Execute the privacy program in functional areas and activities under their responsibility.
  - Ensure that Privacy Act records collected and maintained within the Command or agency are properly described in a Privacy Act system of record notice.

Responsibilities (cont.)

- **Ensure:**
  - No undeclared system of records are being maintained.
  - A Privacy Act Statement is provided to individuals when information is collected that will be maintained in a system of record.
  - Each Privacy Act system of record notice within their purview is reviewed biennially.
  - Updated or new System of Record Notices are submitted to the Army Privacy Office.

Responsibilities (cont.)

- **SYSTEM MANAGERS:**
  - Prepare new, amended, or altered Privacy Act system of record notices and submit to Command Privacy Officer for review.
- **Ensure:**
  - Appropriate procedures and safeguards are developed, implemented, and maintained.
  - All personnel with access to each system are award of their responsibilities for protecting personal information being collected and maintained under the Privacy Act.
  - Each SORN within their area of responsibility is reviewed biennially.

    (http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.aspx)

SORN Review/Update

- Download copy of published SORN into word doc from www.defenselink.mil/privacy/notices/army

- Review and edit the 18 categories of the SORN

SORN Categories

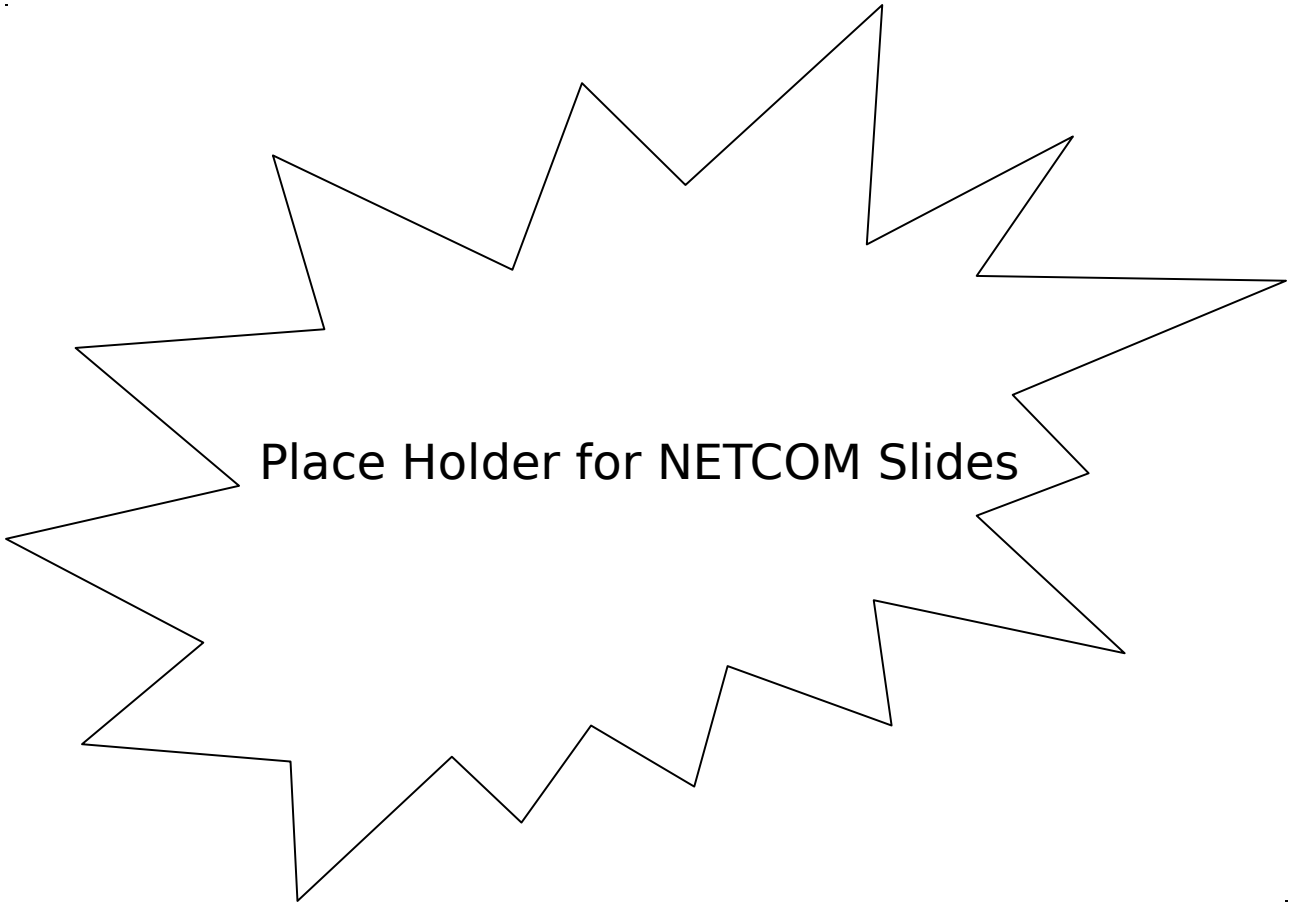
https://www.rmda.army.mil/privacy/docs/foia-sorn.pdf

1. System identifier
2. System name
3. System location
4. Categories of individuals covered by the system
5. Categories of records in the system
6. Authority for maintenance of the system
7. Purpose(s)
8. Routine uses
9. Storage
10. Retrievability
11. Safeguards
12. Retention and disposal
13. System manager(s) and address
14. Notification procedures
15. Record access procedures
16. Contesting record procedures
17. Record source categories
18. Exemptions claimed for the system

System of Record Notice

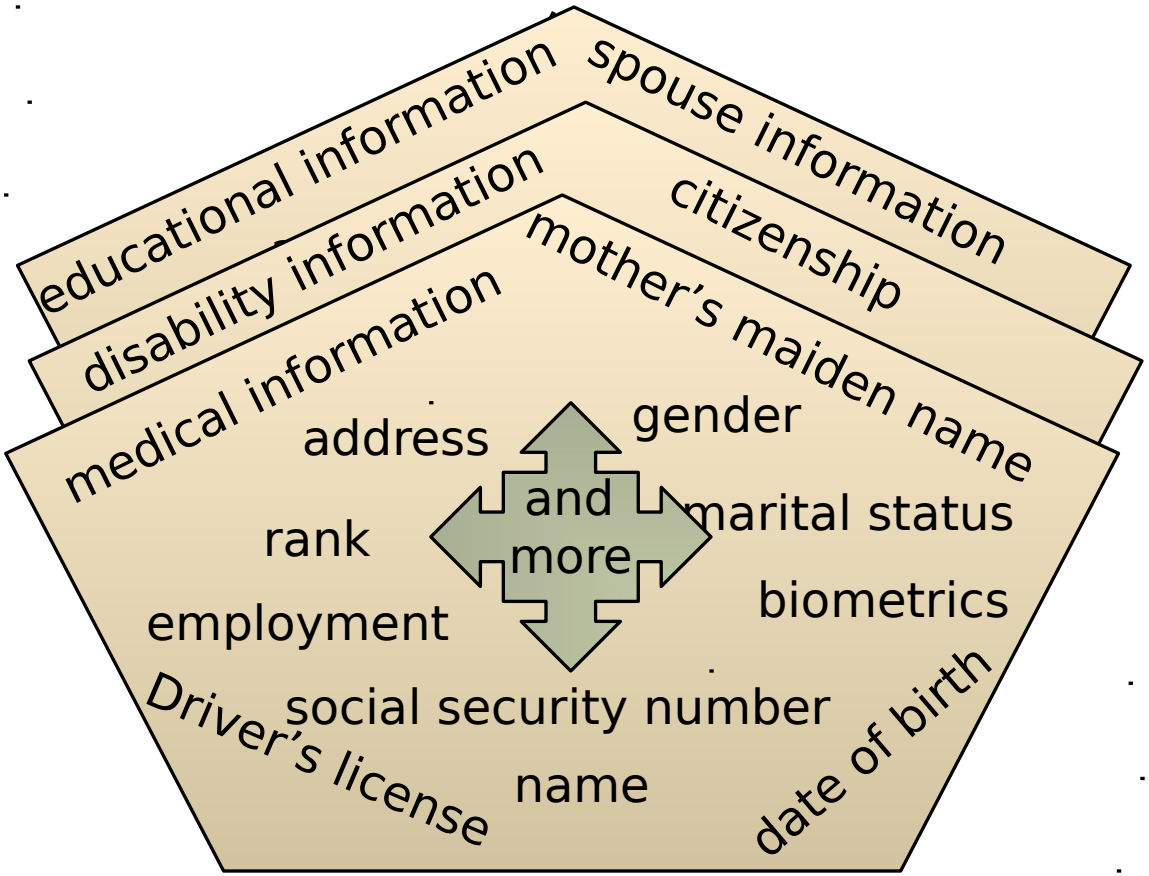
- Privacy Act System of Records Notices (SORNS)
  - Required Documentation
    - ✓ Additions
      Narrative statement and SORN
    - ✓ Alterations
      - Narrative statement, proposed changes to existing
      - SORN, and SORN with changes incorporated
    - ✓ Amendments
      - SORN with proposed changes and SORN with the changes incorporated
    - ✓ Deletions
      - Preamble and notice to request SORN deletion
      - Include what happened to the existing records
      - If now covered under another SORN state which one
    - ✓ Exemptions (submitted with additions or alterations)
      - Documentation that your Office of General Counsel (OGC) or legal section has reviewed and agrees with exemption

Accreditation and FISMA



Personally Identifiable Information (PII)

What is Personally Identifiable Information?



Personally Identifiable Information (PII)

Definition of PII

- **Personally Identifiable Information (PII)**
  - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone;
  - Or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Purpose of the PIA

- **To analyze how PII is handled in order to:**
  - Determine conformance with applicable legal, regulatory, and policy requirements regarding privacy
  - Assess the risks and effects of collecting, maintaining and disseminating PII
  - Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

When is a PIA required?

- System that collect, maintain, use, or disseminate PII on the general public, federal personnel (government civilians, members of the military, and Non-appropriated fund employees), contractors, and Foreign Nationals employed on military bases overseas;

- Prior to developing or purchasing new DoD information or electronic systems, (this includes DoD information systems and electronic collections supported through contracts with external sources that collect, maintain, use, or disseminate PII);

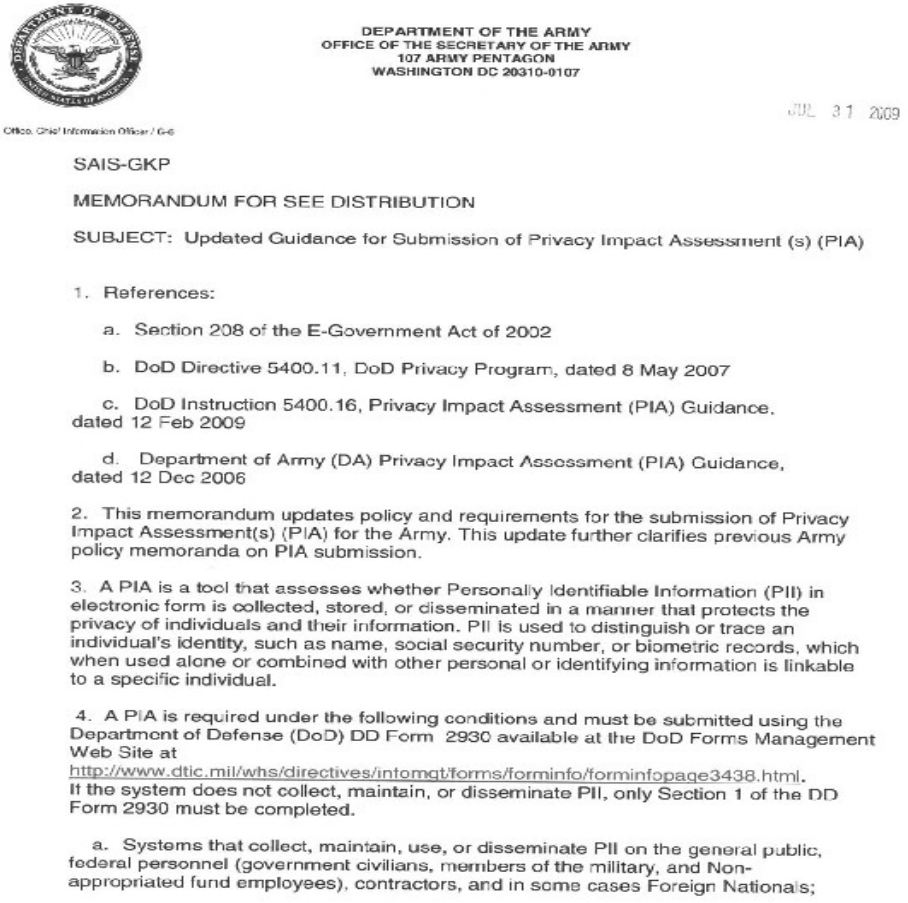
- There is a significant change to a system, to include new application functionalities or changes in privacy risk;

- For legacy systems;

- When converting from paper-based records that contain PII to an electronic system.

Privacy Impact Assessments (PIAs)

CIO/G-6 New Process



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

JUL 31 2009

SAIS-GKP

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Updated Guidance for Submission of Privacy Impact Assessment (s) (PIA)

1. References:

a. Section 208 of the E-Government Act of 2002

b. DoD Directive 5400.11, DoD Privacy Program, dated 8 May 2007

c. DoD Instruction 5400.16, Privacy Impact Assessment (PIA) Guidance, dated 12 Feb 2009

d. Department of Army (DA) Privacy Impact Assessment (PIA) Guidance, dated 12 Dec 2006

2. This memorandum updates policy and requirements for the submission of Privacy Impact Assessment(s) (PIA) for the Army. This update further clarifies previous Army policy memoranda on PIA submission.

3. A PIA is a tool that assesses whether Personally Identifiable Information (PII) in electronic form is collected, stored, or disseminated in a manner that protects the privacy of individuals and their information. PII is used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, which when used alone or combined with other personal or identifying information is linkable to a specific individual.

4. A PIA is required under the following conditions and must be submitted using the Department of Defense (DoD) DD Form 2930 available at the DoD Forms Management Web Site at http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage3438.html. If the system does not collect, maintain, or disseminate PII, only Section 1 of the DD Form 2930 must be completed.

a. Systems that collect, maintain, use, or disseminate PII on the general public, federal personnel (government civilians, members of the military, and Non-appropriated fund employees), contractors, and in some cases Foreign Nationals;

- References
- Updates previous policies
- PIA tool , and various forms of PII data
- New DD Form 2930 and web site for new form location
- PIA update process
- PIA SORN(s)
- When a PIA is not required
- PIA and Privacy Office POCs

PIA REQUIREMENTS OVERVIEW

- Must be submitted on New form – DD Form 2930

- PIAs must be reviewed and updated every three years in conjunction with the Certification and Accreditation (C&A) cycle as a component of the DoD Information Assurance Certification and Accreditation Process (DIACAP) package.

- A System of Records Notice (SORN), is required if a group of files (paper or electronic) are retrieved by name, date of birth, social security number, contains a personal identifier assigned to an individual. (This is misplaced since talking next chart)

- The authorities in the PIA and the SORN should be consistent (use this instead)

Privacy Impact Assessments (PIAs)

PIA

Department of Defense DD Form 2930:
https://www.rmda.army.mil/privacy/docs/dd293PIATemplate.pdf

Template Instruction:
https://www.rmda.army.mil/privacy/docs/Army_PIA_Template_Guidance.pdf

PIA Template

PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enter DoD Information System/Electronic Collection Name
Enter DoD Component Name

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

PIA Template con't

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☐ Yes, DITPR — Enter DITPR System Identification Number
- ☐ Yes, SIPRNET — Enter SIPRNET Identification Number
- ☐ No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ Yes
- ☐ No

If "Yes," enter UPI: 007-21-01-16-02-3116-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☐ Yes
- ☐ No

If "Yes," enter Privacy Act SORN Identifier: AAFES 0405.11

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

PIA Template con't

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

DD FORM 2930 NOV 2008

Page 3 of 15

PIA Template con't

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

- ☐ **Within the DoD Component.**
  Specify.
- ☐ **Other DoD Components.**
  Specify.
- ☐ **Other Federal Agencies.**
  Specify.
- ☐ **State and Local Agencies.**
  Specify.
- ☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)
  Specify.
- ☐ **Other** (e.g., commercial providers, colleges).
  Specify.

PIA Template con't

i. Do individuals have the opportunity to object to the collection of their PII?

☐ Yes ☐ No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ Yes ☐ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

PIA Template con't

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement**	☐ **Privacy Advisory**
☐ **Other**	☐ **None**

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

PIA Template con't

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☐ Name	☐ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☐ Gender
☐ Race/Ethnicity	☐ Birth Date	☐ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☐ Other

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Describe here.

DD FORM 2930 NOV 2008 Page 7 of 15

PIA Template con't

(3) How will the information be collected? Indicate all that apply.

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☐	**Information Sharing - System to System**		
☐	**Other**		

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Describe here.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe here.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☐ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

DD FORM 2930 NOV 2008 Page 8 of 15

PIA Template con't

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☐ Users ☐ Developers ☐ System Administrators ☐ Contractors

☐ Other

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐ Security Guards	☐ Cipher Locks
☐ Identification Badges	☐ Combination Locks
☐ Key Cards	☐ Closed Circuit TV (CCTV)
☐ Safes	☐ Other

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

☐ User Identification	☐ Biometrics
☐ Password	☐ Firewall
☐ Intrusion Detection System (IDS)	☐ Virtual Private Network (VPN)
☐ Encryption	☐ DoD Public Key Infrastructure Certificates
☐ External Certificate Authority (CA) Certificate	☐ Common Access Card (CAC)

☐ Other

If "Other," specify here.

PIA Template con't

(3) Administrative Controls. Indicate all that apply.

- ☐ Periodic Security Audits
- ☐ Regular Monitoring of Users' Security Practices
- ☐ Methods to Ensure Only Authorized Personnel Access to PII
- ☐ Encryption of Backups Containing Sensitive Data
- ☐ Backups Secured Off-site
- ☐ Other

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☐ Yes. Indicate the certification and accreditation status:

☐	Authorization to Operate (ATO)	Date Granted:
☐	Interim Authorization to Operate (IATO)	Date Granted:
☐	Denial of Authorization to Operate (DATO)	Date Granted:
☐	Interim Authorization to Test (IATT)	Date Granted:

☐ No, this DoD information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Describe here.

PIA Template con't

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe here.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.

PIA Template con't

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

PIA Template con't

Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Privacy Officer Signature	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

PIA Template con't

Component CIO Signature (Reviewing Official)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

PIA Template con't

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

After PIA is Approved and Signe

- **Office of Army CIO will:**
  - Send a signed copy to the command
  - Update the Army CIO web site list of approved PIAs
  - Send a copy to ASD NII (who will send to OMB –if on Public)
  - Maintain an electronic and hard copy file of all approved PIAs
  - Update the DITPR-DOA and ask command to review and update as necessary

Privacy Impact Assessments (PIAs)

Your Thoughts, Questions and Recommendations